IN THE CLAIMS:

Please amend claims 1, 2, 4-10, 13-15, 17-19, and 21-23 as follows:

1. (Currently Amended) A method for secured transfer of an N-byte data element from a first memory containing the data element to a second memory through a data bus that is connected between the first memory and the second memory, said method comprising the steps of:

randomly choosing the value of at least one parameter of ~~defining~~ a transfer rule ~~having at least one parameter whose value is chosen at random~~ before each transfer of the N-byte data element, the transfer rule defining the order in which the bytes of the N-byte data element are transferred through the data bus; and

transferring the N-byte data element byte-by-byte through the data bus in ~~accordance with~~ the order specified by the transfer rule, with each byte transiting once and only once through the data bus.

2. (Currently Amended) The method as defined in claim 1, wherein the transfer rule is a permutation of the bytes of the N-byte data element such that each transfer of the N-byte data element is not done in the same byte order.

3. (Original) The method as defined in claim 2, wherein the permutation is defined by the relationship:

$X = (X0 + DIRECTION * PITCH * j)$ modulo N,

where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, X0 ranges from 0 to N-1, and j varies from 0 to N-1.

4. (Currently Amended) The method as defined in claim 3, wherein in the ~~defining~~ step of randomly choosing, the value of PITCH is chosen randomly before each transfer of the data element.

5. (Currently Amended) The method as defined in claim 4, wherein in the ~~defining~~ step of randomly choosing, the value of DIRECTION is chosen randomly before each transfer of the data element.

6. (Currently Amended) The method as defined in claim 5, wherein in the ~~defining~~ step of randomly choosing, the value of X0 is chosen randomly before each transfer of the data element.

7. (Currently Amended) The method as defined in claim 3, wherein in the ~~defining~~ step of randomly choosing, the value of DIRECTION is chosen randomly before each transfer of the data element.

8. (Currently Amended) The method as defined in claim 7, wherein in the ~~defining~~ step of randomly choosing, the value of X0 is chosen randomly before each transfer of the data element.

9. (Currently Amended) The method as defined in claim 3, wherein in the ~~defining~~ step of randomly choosing, the value of X0 is chosen randomly before each transfer of the data element.

10. (Currently Amended) The method as defined in claim 3, wherein in the ~~defining~~ step of randomly choosing, the value of PITCH and the value of X0 are chosen randomly before each transfer of the data element.

11. (Original) The method as defined in claim 3, wherein PITCH and N are mutually prime numbers.

12. (Original) The method as defined in claim 3, wherein N is a prime integer and PITCH is an integer ranging from 1 to N-1.

13. (Currently Amended) The method as defined in claim 3,
wherein the ~~defining~~ step of randomly choosing includes the sub-steps of:

determining the values of PITCH, DIRECTION, and X0, the value of at least one of PITCH, DIRECTION, and X0 being randomly chosen; and

initializing j and X, and

the transferring step includes the sub-step of repeating N times the steps of:

reading a byte of the data element from the first memory, the place value of the byte read being equal to the current index (X);

writing in the second memory the byte that was read from the first memory; and

incrementing j and varying X.

14. (Currently Amended) A machine-readable medium encoded with a program for secured transfer of an N-byte data element from a first memory containing the data element to a second memory through a data bus that is connected between the first memory and the second memory, said program containing instructions for performing the steps of:

randomly choosing the value of at least one parameter of ~~defining~~ a transfer rule ~~having at least one parameter whose value is chosen at random~~ before each transfer of the N-byte data element, the transfer rule defining the order in which the bytes of the N-byte data element are transferred through the data bus; and

transferring the N-byte data element byte-by-byte through the data bus in ~~accordance with~~ the order specified by the transfer rule, with each byte transiting once and only once through the data bus.

15. (Currently Amended) The machine-readable medium as defined in claim 14, wherein the transfer rule is a permutation of the bytes of the N-byte data element such that each transfer of the N-byte data element is not done in the same byte order.

16. (Original) The machine-readable medium as defined in claim 15, wherein the permutation is defined by the relationship:

X = (X0 + DIRECTION * PITCH * j) modulo N,

where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, X0 ranges from 0 to N-1, and j varies from 0 to N-1.

17. (Currently Amended) The machine-readable medium as defined in claim 16, wherein in the ~~defining~~ step of randomly choosing, the value of PITCH is chosen randomly before each transfer of the data element.

18. (Currently Amended) The machine-readable medium as defined in claim 16, wherein in the ~~defining~~ step of randomly choosing, the value of DIRECTION is chosen randomly before each transfer of the data element.

19. (Currently Amended) The machine-readable medium as defined in claim 16, wherein in the ~~defining~~ step of randomly choosing, the value of X0 is chosen randomly before each transfer of the data element.

20. (Original) The machine-readable medium as defined in claim 16, wherein PITCH and N are mutually prime numbers.

21. (Currently Amended) The machine-readable medium as defined in claim 16,

wherein the ~~defining~~ step of randomly choosing includes the following sub-steps:

determining the values of PITCH, DIRECTION, and X0, the value of at least one of PITCH, DIRECTION, and X0 being randomly chosen; and

initializing j and X, and

the transferring step includes the sub-step of repeating N times the steps of:

reading a byte of the data element from the first memory, the place value of the byte read being equal to the current index (X);

writing in the second memory the byte that was read from the first memory; and

incrementing j and varying X.

22. (Currently Amended) A programmable circuit comprising:

a data bus;

a read-only memory containing an N-byte data element to be transferred, the read-only memory being coupled to the data bus;

a writable memory coupled to the data bus;

a control unit coupled to the read-only memory and the writable memory; and

a random number generator coupled to the control unit, the random number generator supplying the value of at least one parameter of a data transfer rule ~~that is used to~~ before each transfer of the N-byte data element from the read-only memory to the writable memory, the data transfer rule defining the order in which the bytes of the N-byte data element are transferred through the data bus,

wherein the control unit controls the data bus such that ~~bytes of~~ the N-byte data element ~~transit~~ is transferred byte-by-byte through the data bus in the order specified by the data transfer rule, with each byte transiting once and only once through the data bus~~, and the at least one parameter is supplied by the random number generator for each transfer of the data element~~.

23. (Currently Amended) The programmable circuit as defined in claim 22, wherein the data transfer rule is a permutation of the bytes of the N-byte data element such that each transfer of the N-byte data element is not done in the same byte order.

24. (Original) The programmable circuit as defined in claim 23, wherein the permutation is defined by the relationship:

$X = (X0 + DIRECTION * PITCH * j)$ modulo N,

where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, X0 ranges from 0 to N-1, and j varies from 0 to N-1.